Privacy in IoT

The unique opportunity to learn and discuss where the Internet of Things meets GDPR, and where Hyperconnectivity meets Privacy & Security. Who wouldn't be totally confused!? In our Open Webinars, Arthur’s Legal will address the Pains & Gains of the GDPR, X By Design & Resilience.

Arthur van der Wees
Dimitra Stefanatou
Janneke Breeuwsma

Arthur’s Legal organizes seven (7) webinars on Privacy in IoT with the focus on GDPR, supported by AIOTI and Create-IoT

Go to arthurslegal.com/iot/ for more information and subscription for the webinars.
Privacy in IoT

Open Webinars by Arthur’s Legal, supported by:
AIOTI WG3 Privacy-in-IoT Taskforce, and
H2020 CSA CREATE-IoT & LSPs AG Trust in IoT

Arthur van der Wees
Managing Director Arthur’s Legal, the global tech-by-design law firm & strategic knowledge partner
Expert Advisor to the European Commission (Cloud, IoT, Data Value Chain, Cybersecurity, Privacy & Accountability)
Project Leader H2020 IoT LSPs & CSAs Activity Group on Trust, Security, Privacy, Accountability & Liability
Founding Member, EC’s Alliance for IoT Innovation (AIOTI)
Task Force Leader AIOTI Security in IoT & Privacy in IoT
Privacy in IoT Open Webinar Series

Webinar 1: GDPR: Processing, Protection, Security & Strategies
Webinar 2: X-by-Design: Upstream & Downstream Resilience
Webinar 3: State of the Art Privacy Principles & Requirements Right Now!

Webinar 4: Consent Management & Engagement in IoT
Wednesday 2 May 2018, 10.00 - 11.00 CET

Webinar 5: Compliance, Accountability, Assurance & Penalties
Wednesday 9 May 2018, 10.00 - 11.00 CET

Webinar 6: IoT Ecosystems, Pre-Procurement & Collaboration
Wednesday 16 May 2018, 10.00 - 11.00 CET

Webinar 7: Data Subject Rights & Data Management in IoT
Wednesday 23 May 2018, 10.00 - 11.00 CET

Please subscribe to the Privacy in IoT Mailing List at: www.arthurslegal.com/IoT, in which we will keep you up to date with dates, login details and the latest news on the GDPR, Privacy in IoT and related topics.
Webinar Nr. 3

SOTA

State of the Art Privacy Principles & Requirements
‘We are in a position today, in this Digital Age, where Technology has outstripped our Legal Framework’

Admiral Michael Rogers, Director NSA & Commander CYBERCOM
From 2018, Digital & Data become Highly Regulated Domains

- **PSD2**: 13 January 2018
- **NIS**: 9 May 2018 (Identifying operators of ‘Essential Services’ 9 November 2018)
- **GDPR**: 25 May 2018
- **Trade Secrets Directive**: 9 June 2018
- **e-Privacy Regulation (draft)**
- **Free Flow of Data Regulation (draft)**
- **Cyber Security Act & Certification Scheme (draft)**
- **Public Services Information Directive (revision)**

1 January 2018
30 Days to Effective Date GDPR
25 May 2018

All rights reserved, Arthur's Legal B.V.
The GDPR is not reinventing the wheel ...
Changes GDPR (Part 3 of 7)

Appropriate Personal Data Security Measures:

Appropriate Technical & Organizational Measures, Pseudonymisation & Encryption, Confidentiality, Integrity, Availability, Transparency, Isolation (Purpose Limitation), Data Intervenability, Monitoring & Evaluation
What Can We Do?

What Should We Do?
A. Technical Measures
B. Organisational Measures
C. Policies & Documentation
All Markets Are Dynamic
#SOTA
State of The Art
Malicious Actors Are Not Into State of Play

State of the Art
By Default & Daily Need
State of the Art

= Principle-Based + Risk- & Impact-Based + Dynamic & Continuous
Principles & Requirements

Mandatory & Voluntary
GDPR = GPDPMPS Regulation

Personal Data Collecting & Other Processing
Personal Data Protection & Security
Personal Data Management
First Privacy Principle in IoT

No Personal Data by Default

Avoid Personal Data (PII) Collection or Creation (*)

(*) Exceptions permitted, when & where required
Second Privacy Principle in IoT

‘As If’ X-By-Design

Design & Engineer Ecosystems As-If these will (now or in a later phase) process Personal Data

Privacy & Security By Default & By Design
Privacy by Default

vs

Security by Default
Privacy & Security Principles in IoT

Data Minimisation
Privacy & Security Principles in IoT

Purpose Limitation

No legal ground or legitimate interest under the GDPR, no more data processing
De-Identifying & Data Deletion

The fine balance between immediate strong deletion when no legal ground and legitimate purpose under the GDPR is available, and mandatory retention obligations by the data controller/processor.
Privacy & Security Principles in IoT

Transparency

A data subject should be able to know who is taking what action with its personal data
Privacy & Security Principles in IoT

**Data Control**

A data subject should at all times be able to have control over its personal data.
Accountability

Any data controller/processor is accountable for regulatory and contractual compliance to the extent concerning its level of collecting, using, sharing and other processing, the related impact assessment linked to technical and operational measures, including with and for data subcontractors involved. Accountability can not be outsourced.
Minimise Fragmentation

IoT SDOs and Alliances Landscape
(Technology and Marketing Dimensions)

Source: AIOTI WG3 (IoT Standardisation) – Release 2.7
Build Your Own SOTA Security in IoT Model
It’s Easy; Just Think N-Dimensional!

1. 35+ SOTA Security Recommendations, Frameworks & Guidelines
2. 1,000+ Security Requirements & Principles (450+ Unique)
3. Segmentation into 4 Layers & 3 Dimensions
4. Structure, Systemize & Semantic Sanitization without Interpretation
5. Context (initially: each of the 5 LSPs)
6. Stakeholders (User, Customer, Supplier, Policy Makers, SDO, Authorities)
7. 5 Life Cycle Methodologies (Device, Data, Stakeholder, Context, Legal)
8. Interdependencies & Double-Looping
GDPR Stakeholders

- Data Subject
- Data Controller
- Data Processor
- Data Protection Authority
- Other Data Actors
Human-Centric Technology, Thriving Ecosystems & Multi-Angled Stakeholders & Influencers

1. The **User** (Convenience-Focused, Cheap, Curious, Creative, Ignorant)
2. **Customers** Who Are Willing To Pay(B2x, x2x)
3. **Suppliers & Value Ecosystem** (Secure In, Secure Inside, Secure Out)
4. Thriving **Ecosystems & Society**
5. **Malicious Actors** (They Are Patient. And They Collaborate! We Do Not)
6. Act First Seek Forgiveness Later **Data Brokers**
7. **Policy** Makers, **Standardisation** Development Orgs & Markets
8. **Authorities** (Who is responsible for what, and are they capable?)
9. **Data Access**: Law Enforcement & Intelligence Services
General IoT Layered SOTA Plotting Methodology: Dimensions & Layers

1. User & Human Factor
2. Data
3. Identity & Authentication
4. Service
5. Software & Application
6. Hardware
7. Infrastructure & Network
7 Phases of the (Personal) Data Life Cycle

1. Obtain / Collect
2. Create / Derive
3. Use
4. Store
5. Share / Disclose
6. Archive
7. Destroy / Delete

Most PII* comes out of Phase 1 & 2
BUT
Personal Data is created & processed in any and each phase

Which phase(s) are we talking about?
PII* + Actor + Legal Basis + Purpose(s)

* PII: personal identified or identifiable information
Privacy & Security Principles in IoT

Continuous SOTA Security
The GDPR offers an equation for finding the appropriate level of protection, per purpose, per impact assessment, and per economic feasibility. See the Articles 25 & 32 GDPR. We call this the \textit{Appropriate Dynamic Accountability (ADA) Formula}:

\textbf{State of the Art Security – Costs – Purposes + Impact}

Although the current information security standards aim for ‘achieving continual improvement’, the GDPR aims to ensure up-to-date levels of protection by requiring the levels of data protection and security to continuously meet the ADA formula.
From Continual to Continuous State of the Art Security

Although the current information security standards aim for ‘achieving continual improvement’, articles 25 and 32 GDPR aims to ensure up-to-date levels of protection by requiring the levels of data protection and security to continuously meet the Appropriate Dynamic Accountability (ADA) Formula.
Security & Privacy in IoT / State of the Art (SOTA)

12. United States Department of Health and Human Services, Food and Drug Administration: Content of Premarket Submissions for Management of Cybersecurity in Medical Devices
35 +

US Congress Proposal for IoT Cybersecurity Improvement Act (2017)
OWASP IoT Framework Assessment (2018)
Security in IoT / State of the Art (SOTA)

EC/AIOTI Reports on Workshops on Security and Privacy in IoT

AIOTI Workshop on Security and Privacy in IoT of June 2016:

Final Report Workshop on Security and Privacy in IoT of June 2016:

Final Report European Commission of January 2017 Workshop on Internet of Things Privacy and Security:

IERC IoT Handbook Paragraph 6.3.3:
### Snapshot Example

#### SOTA Security Plotting

<table>
<thead>
<tr>
<th></th>
<th>10.1</th>
<th>10.2</th>
<th>10.3</th>
<th>10.4</th>
<th>10.5</th>
</tr>
</thead>
<tbody>
<tr>
<td>287</td>
<td>Network authentication</td>
<td></td>
<td></td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>288</td>
<td>Device and owner authentication</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>289</td>
<td>Utilize a trust anchor</td>
<td></td>
<td></td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>290</td>
<td>Use a tamper resistant trust anchor</td>
<td></td>
<td></td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>291</td>
<td>Enforce confidentiality and integrity to/from the trust anchor</td>
<td></td>
<td></td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>292</td>
<td>Perfect Forward Secrecy (PFS)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>293</td>
<td>Force authentication through the service ecosystem</td>
<td></td>
<td></td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>294</td>
<td>Define application layer authentication and authorisation</td>
<td></td>
<td></td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>295</td>
<td>Define an organizational root of trust</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>296</td>
<td>Define a communications model</td>
<td></td>
<td></td>
<td>Y</td>
<td></td>
</tr>
</tbody>
</table>

10.01 GSMA: IoT Security Overview Document  
10.02 GSMA: IoT Security Guidelines for IoT Service Ecosystem  
10.03 GSMA: IoT Security Endpoint Ecosystems  
10.04 GSMA: IoT Security Guidelines for Network Operators  
10.05 GSMA: IoT Security Assessment Framework
Contextuality
Use Case: Smart Carpets

www.activageproject.eu
General State of The Art SOTA IoT Plotting Methodology

1. User/Human Factor
2. Data
3. Service
4. Software/Application
5. Hardware
6. Authentication
7. Infrastructure/Network
Use Case 1: Smart Carpet Sensors for Aging Well
Use Case 1: Smart Carpet Sensors for Aging Well
Use Case 1: Smart Carpet Sensors for Aging Well

1. USER/HUMAN FACTOR
   1. Basic principles:
      1. Human-centric approach: Security and privacy should be universally applied to all users.
      2. Privacy by design: Privacy of users must be embedded into the design of business processes, technologies, operations and information architectures. Each service or business process designed to use personal data must take all the necessary security requirements into consideration at the initial stages of their developments. Privacy must be embedded into the design of business processes, technologies, operations and information architectures.
      3. Privacy by default: The strictest privacy settings and mechanisms must automatically apply once a user acquires a new product or service; no manual change to the privacy settings should be required on the part of the user.
      4. Decoupling multiple identities: It should be easy to decouple multiple personae of the users from one another.
   2. User’s awareness and control:
      1. Transparency of data processing: The service provider should empower users to know what the devices are doing and what personal data they are sharing and why, even if it concerns M2M communications and transactions.
      2. Transparency of privacy policy: The service provider should ensure that the user is and remains clear and aware of privacy issues, choices it makes and possible consequences thereof.
   3. Handling of personal data:
      1. Non-discriminatory practices: The service provider should ensure non-discriminatory practices against users and businesses on the basis of information derived from IoT deployments (e.g. within smart cities).
      2. Manufacturer-implemented parametrization: By design, the user should be able to configure and manage rights for accessing data controlled by them based on the assessment where (in its lifecycle) the device comes into contact with personal data, creates/derives (new) personal data, or otherwise processes personal data, while keeping in mind the contextuality of purposes and use, as well as multi-purpose Things and IoT ecosystems.
      3. Accountability: Any service provider should be accountable for regulatory, contractual and ethical compliance.
Use Case 1: Smart Carpet for Aging Well

6. AUTHENTICATION
   Location authentication
   Network authentication

7. INFRASTRUCTURE/NETWORK
   System tests & assurance
Multi-Layered Cross-Cutting Interdisciplinary Integrated Architecture

Functionality, Interface & UI
SOTA Security & Safety
Identities, Authentication & Access
SOTA (Personal) Data Protection
Data Right Management & Analytics
Sustainability & Economic Feasibility

Multi-Layered, Cross-Cutting Interdisciplinary Integrated High-Level Architecture

Usability, Transparency, Trust, Control & Compliance Inside = Success By Design

All rights reserved, Arthur's Legal B.V.
Man & Technology Symbiosis: Hyperconnectivity!

Q&A: Anything Goes!

vanderwees@arthurslegal.com

Arthurslegal.com
@Arthurslegal
Arthur’s Legal: Arthur’s Legal a global tech and strategic x-by-design law firm. Arthur’s Legal is founded in 2001 and since its incorporation provides integrated full services, and mainly focuses on local and global private and public organizations that are active as customer, user, vendor, integrator, consultant, legislator or policy maker in the fields of IT, licensing, cloud computing, internet of things, data analytics, cybersecurity, robotics, distributed ledger (block chain) technology and artificial intelligence.Arthur’s Legal is also a leading deal making expert; it has already structured and negotiated out more than 5,000 major technology and related deals with and for global Fortune companies as well as other major organizations in the public and private sector worldwide.

Arthur’s Global Digital Strategies: The counsels of Arthur’s Legal are legal experts, strategists, technologists, standardization specialists and frequent speakers worldwide, with in-depth experience and are well-connected in the world of technology, combinatoric innovation, data, digital, cybersecurity, (personal) data protection, standardization, risk management & global business. On these topics, its managing director Arthur van der Wees LLM is expert advisor to the European Commission, Dutch government as well as other public and private sector organizations and institutes worldwide.

Trust, Digital Data, Cybersecurity, Algorithms, AI, Robotics & Internet of Things: Arthur’s Legal is Founding Member of European Commission’s (EC) Alliance of IoT Innovation (AIOTI), Co-Leader of AIOTI WG4 (Policy), Project Leader of both the AIOTI Security in IoT and Privacy in IoT taskforces, co-author of EC’s Cloud SLA Standardisation Guidelines, co-author of Cloud Security Alliance’s Privacy Level Agreement (PLA) 2.0, co-contributor to ISO standards such as ISO/IEC 19086 (Cloud Computing), co-author of the IERC Handbooks 2016 (Strategic & Legal Challenges in IoT) and 2017 (Security & Privacy in IoT), member of ESCO and co-author of the Dutch National Smart Cities’ Strategy. Arthur’s Legal is co-founder of CloudQuadrants on the maturity of cloud offerings, the Cyberchess Institute that landscapes the real-life cybersecurity arena, the Cyber Trust Institute that sets trust trajectories and orbital requirements and parameters for technology-as-a-service, the Institute for Next Generation Compliance that promotes the restructuring and automation of compliance and related procurement, and the Institute for Data and Evidence Based Trust that aims to build and enhance trust and data protection in open, decentralized digital, cyber-physical and virtual ecosystems. Furthermore, Arthur’s Legal is EC H2020 project IoT CREATE consortium partner and activity group leader on trust, security, safety, privacy, legal and compliance topics in IoT in five EU large scale pilots on smart healthcare, smart cities, wearable, smart farming, food safety and autonomous vehicles with EUR 250M of accrued EC and other funding. Together with IDC Arthur’s Legal is also doing research and policy making for the Commission on data portability & application portability. One can build it’s own AI with Zapplied.

Connected & Hyper-connected: Arthur’s Legal has an unique interdisciplinary 3D-angle & x-by-design approach, connecting vital topics such as usability, security, data management, (personal) data protection, compliance with technology, infrastructure, architecture and global standardization thereof, with the capability and ability to connect those components in hyper-connected ecosystems much earlier (read: pro-active, preventative) than the traditional policy-making, legal and compliance practice does. For upcoming events, key notes and other activities, please check out website, stay up to date via its social media channels, or contact us.

www.arthurslegal.com | vanderwees@arthurslegal.com
Trustworthy Internet
of Everything & Everybody
for the Wellbeing of People and Planet

Legal Notices

All rights reserved, Arthur’s Legal. The content of this document is provided ‘as-is’ and for general information purposes only; it does not constitute strategic, legal or any other professional advice. The content or parts thereof may not be complete, accurate or up to date. Notwithstanding anything contained in this document, Arthur’s Legal disclaims responsibility (including where Arthur’s Legal or any of its officers, employees or contractors have been negligent) for any direct or indirect loss, damage, claim, or liability any person, company, organisation or other entity or body may incur as a result, this to the maximum extent permitted by law.